Digital Energy

Patch Validation Program for Power Generators Cyber Security Solutions

SIMPLIFY OT MAINTENANCE AND IMPROVE SECURITY

How can you stay on top of all the patches available and deploy them fast—without breaking your operations or budget? With the Patch Validation Program from GE's Digital Energy, you can harness comprehensive patch management services that fuel optimized security, reliability, and operational efficiency.

BUSINESS CHALLENGES

$243 billion – $1 trillion: Impact to the US economy of an electricity blackout across 15 US states affecting 93 million people.[1]

64% of power and utilities believe that their security strategy is not aligned with today's risk environment.[2]

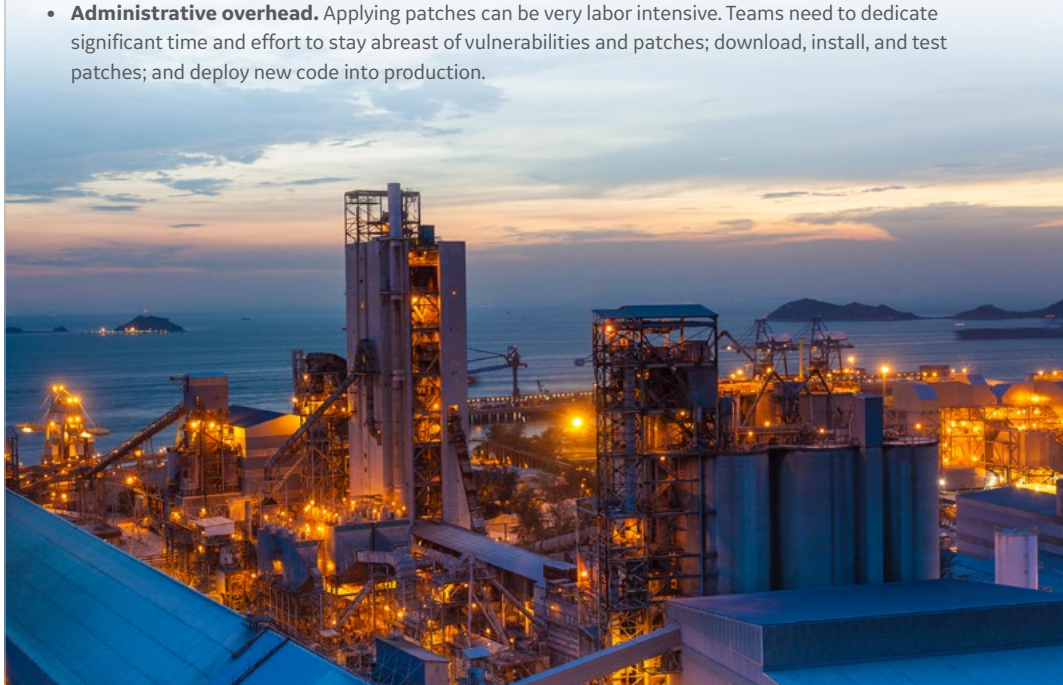
$3.86 million: Average total cost of a data breach.[3]

OVERVIEW

Contending with the Challenges of Patch Management

For operators and owners of power generation systems, ensuring compliance and guarding against evolving cyber security threats represent critical, continuous imperatives. Toward that end, it's vital to quickly apply patches and fixes when vulnerabilities are identified. However, for resource-constrained operations teams, these patch validation, testing, and deployment efforts can present a number of challenges:

- **Risk.** Patches can address vulnerabilities but they can also introduce performance and availability issues when they are deployed in production environments—jeopardizing critical power systems and services.
- **Complexity.** Staying on top of vulnerabilities and patches available can be difficult. For internal teams, it can be hard to verify which vulnerabilities affect specific environments and how interdependent systems may be affected.
- **Administrative overhead.** Applying patches can be very labor intensive. Teams need to dedicate significant time and effort to stay abreast of vulnerabilities and patches; download, install, and test patches; and deploy new code into production.



ge.com/power/digitalenergy

Patch Validation Program for Power Generators Cyber Security Solutions

Simplify OT Maintenance and Improve Security

Solution Benefits

Put the Patch Validation Program to work for your organization and you can realize the following benefits:

Reduce cyber risk exposure.
This program helps your team more quickly and consistently apply patches and other mitigation tactics, so you can more effectively safeguard your environment and adhere to cyber security best practices.

Enhance compliance.
With this program, you can more consistently and comprehensively comply with a number of government and industry cyber security standards, including North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP), Nuclear Energy Institute (NEI) 08-09, and ISA 99/IEC 62443.

Maximize system availability.
By employing the program's validated, pre-packaged updates, your organization can avoid the potential risks of implementing patches that can have a negative impact on production environments.

Boost operational efficiency.
By harnessing these services, your internal teams can reduce the time they spend on laborious efforts like patch testing. Plus, they can deploy tested and validated patches that have been proven to run in a similar environment—and so minimize the trial, error, and remediation efforts associated with implementing untested patches.

Solution Introduction

Now, your organization can gain the security and compliance benefits of optimized patch management capabilities, while offloading a lot of the effort and risk associated with handling these efforts internally—with the Patch Validation Program. This program offers comprehensive patch management services that promote the availability, integrity, and confidentiality of your critical controls and related networks.

Through this service, we'll deliver the patches you need—in validated, tested, and easy-to-deploy packages. We further support your patch management efforts through cumulative updates, deployment automation, and useful, easily accessible documentation. By employing this service, your organization can mitigate its exposure to cyber risk, maximize the availability of your critical systems, and boost operational efficiency.

Key Features

Testing and Validation

As part of the program, GE will test and validate antivirus (AV) and host intrusion detection (HID) signature updates as well as operating system (OS) patches. First, we'll verify whether these new releases apply to your environment, and based on that, we'll establish a list of candidates for testing.

GE's staff then test applicable updates in controlled, representative lab environments that offer safeguards against intrusion and tampering. Through this testing, we determine whether updates adversely affect the functional operation of the control system, related interfaces, or system communications. Based on our findings, we can exclude any updates that may introduce performance or availability issues. Further, if a given patch is excluded, we provide documentation to support this exclusion.

Patch Packaging and Delivery

Once patches have been tested and validated, we make them available to customers via a secure web portal. We provide cumulative updates so that your organization can stay completely up to date with the latest releases, even if an earlier update wasn't applied. By delivering these complete, scripted packages, we make it easy for your team to incorporate updates into your transfer and change management processes.

Host-Based and Central, Network-Based Deployment Options

The Patch Validation Program is available as a stand-alone offering. Through the program, we deliver scripted files that automate the deployment of patches and antivirus updates. In addition, your organization can deploy these patches using Baseline Security Center. Baseline Security Center brings centralized management to the deployment process, reducing the need to run patch deployment tools locally on each system being patched. By harnessing these combined offerings, your team can enjoy even greater speed and efficiency gains.

Backed by a Commitment to Quality

We employ Six Sigma tools and we empower team members to make customer-focused quality the highest priority. Further, our team participates in a number of external quality certification programs, including ISO-9001:2015 and ISO-27001:2013.

Patch Validation Program for Power Generators Cyber Security Solutions

Simplify OT Maintenance and Improve Security

Service Specifics

Environment Support

- GE's turbine, generator, and plant controls and associated networks
- GE's HMI and Historian hosts, GE's Thin Client HMI / Control Server environments
- Platform Support: Windows 7, Windows Server 2008 R2, Windows Server 2012 R2, and Windows Server 2016

Onsite Training

- GE offers up to eight hours of onsite patch deployment training during the initial implementation period

Patch Validation Program Support

- GE's Product Security Incident Response Team (PSIRT) is responsible for monitoring for cyber-security issues that affect products and coordinating responses. You can report an issue through the PSIRT website at the following URL: www.ge.com/security.

How to Get Started

To learn more and sign up, please contact your local GE's Digital Energy or GE's Power Services Account Executive or call 770-722-2552.

Sources

1 Lloyds, "Emerging Risk Report—2015," May 2015, www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/risk/downloads/crs-lloyds-business-blackout-scenario.pdf.

2 Ernst & Young, "Plug in: EY's latest insights for Power & Utilities," March 2015, www.ey.com/Publication/vwLUAssets/EYs-latest-insights-for-power-utilities/$File/EYs-latest-insights-for-power-utilities.pdf.

3 Ponemon Institute research, sponsored by IBM, "2018 Cost of a Data Breach Study: Global Overview," July 2018, https://databreachcalculator.mybluemix.net/assets/2018_Global_Cost_of_a_Data_Breach_Report.pdf.

Contact Us
www.gepower.com/contact